PCT/EP 9 9 / 1 0 4 0 5 PHD 99002

BUNDESREPUBLIK DEUTSCHLAND

4 EP99/1040S PHD 99001

EPO - DG 1

- 3 03. 2000

REC'D 14 MAR 2000 (63)

PCT

Bescheinigung

09/623643

Die Philips Patentverwaltung GmbH in Hamburg/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Konstantstromregler für Chipkartenschaltungen"

am 7. Januar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Der Firmenname der Anmelderin wurde geändert in:
Philips Corporate Intellectual Property GmbH.

Das angeheftete Stück ist eine richtige und genaue Wiedergabe der ursprünglichen Unterlage dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 06 K und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 1. Februar 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Wehner

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Aktenzeichen: 199 00 261.4

A 9161
06.90
11/98

Konstantstromregler für Chipkartenschaltungen

I Anwendungsgebiet, sowie Beschreibung des Stands der Technik

Anwendungsgebiet sind Chipkarten (Smart Cards), die z.B. als Zahlungsmittel oder als Zugangskontrollen oder zu ähnlichen Zwecken benutzt werden. Diese beinhalten geheime Daten, wie Guthaben oder Schlüssel, die sie zu ihrem Betrieb benötigen.

Es ist nun das Ziel von spezialisierten Einbrechern (Hackern, Ausforschern), diese geheimen Daten ausfindig zu machen, um die Betriebsweise dieser Karten zu erforschen oder um sie nachzumachen oder um sie zu ‚knacken', das heißt das Geheimnis auf der Karte zu erforschen. Dazu bedienen sich solche Ausforscher diverser Mittel. U.a. wird das Muster evaluiert, das die Logik durch ihren Versorgungsstrom auf den Versorgungsleitungen der Schaltung erzeugt. Dabei kann sowohl der Spannungsverlauf, als auch der Stromverlauf evaluiert werden. Aus vielen Abtastungen kann dann unter speziellen Umständen korreliert werden, welche Datenmuster zu einem bestimmten Zeitpunkt in der Karte verarbeitet werden. Wenn diese Evaluierungen überhaupt möglich sind, so sind sehr schwierig auszuführen.

Die 'Differential Power Analysis' ist eine neue Methode, welche es erlaubt, über die reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung zu gewinnen.

Die 'Differential Power Analysis' hat den Ansatz, daß neben den Ein-/Ausgangssignalen zusätzlich
(a) die Stromaufnahme beziehungsweise
(b) Spannungseinbrüche an der Versorgungsspannung der integrierten Schaltung analysiert werden. Diese beiden Informationsquellen werden durch die vorliegende Erfindung eliminiert.

Der Erfolg dieser Analysemethode hängt davon ab, ob man eine Anzahl A von analogen Signalverläufen (entsprechend (a) oder (b)) S(k,t) über die Zeit t mit k={1,...,A} unterschiedlichen Operanden so aufnehmen kann, daß eine Summenbildung der Form

$$T(i,t) = \sum_{k=1}^{A} p(i,k) * S(k,t)$$ mit den Koeffizienten p(i,k), i={0, 1, 2,...}

möglich ist. Betrachtet man unterschiedliche Signalverläufe S(k1,t1), S(k2,t1), S(k3,t1), ... zum gleichen Zeitpunkt t=t1, kann eine 'Differential Power Analysis' nur funktionieren, wenn die integrierte Schaltung in diesem Moment die gleiche Rechenoperation ausführt mit unterschiedlichen Operanden k={1,...,A}, d.h. die Signalverläufe S(k,t) müssen genau übereinandergelegt werden können. Dieses gilt nicht nur für die Berechnung selbst, sondern auch für die Ein- und Ausgabe von Daten.

2 Aufgabe der Erfindung

Was ist zu verbessern

Es ist Aufgabe der vorliegenden Erfindung, Mittel anzugeben, die eine Evaluierung deutlich erschweren, wenn nicht gar unmöglich machen.

Aktuelle Problematik

Die aktuelle Problematik liegt darin, daß die Schaltungen in den Karten synchron getaktet werden und mit Hilfe dieses Taktes streng steuerbar und teilweise auch evaluierbar sind.

3 Erfindungsgemäße Lösung der gestellten Aufgabe

Ein Mittel, das zur Verwirrung bei der unerwünschten Evaluierung dienen kann, besteht darin, daß man innerhalb der Schaltung keine synchrone, getaktete Logik verwendet, sondern asynchrone, ungetaktete Logik. Diese hat die Eigenschaft, auf der Versorgungsleitung ein unkorrelierbares Muster zu erzeugen.

Ferner ist der Zeitpunkt, zu dem eine spezielle Berechnung bitgenau ausgeführt wird, nicht aus dem äußeren Strom- bzw. Spannungsverlauf an der Versorgungsleitung ablesbar.

Es wird eine Schaltung für kontaktlose Chipkarten vorgeschlagen basierend auf den folgenden zwei Subschaltungen:

- Eine Versorgungsquelle mit den folgenden zwei Charakteristiken:
  - am empfangenden Ende ist die Last unabhängig von der Last auf der speisenden Seite,
  - an der speisenden Seite verhält sich die Quelle über einen weiten Bereich wie eine Stromquelle. Solch eine Versorgungsquelle kann konstruiert werden durch einen Parallelregler (Shunt Typ).

  Die kontaktlose Energiespeisung einer Chipkarte weist die Charakteristik einer Konstantstromquelle auf, ohne dabei geregelt werden zu müssen.

- Eine informationsverarbeitende Schaltung, die über einen weiten Bereich der Spannungsversorgung arbeitet, indem sie ihre Verarbeitungsgeschwindigkeit und damit den Datendurchsatz der verfügbaren Versorgungsspannung anpaßt. Solch eine Verarbeitungsschaltung kann erstellt werden durch asynchrone Schaltungen [1], [2], [3]. Diese sind über einen weiten Versorgungsspannungsbereich funktionsfähig bei vergleichsweise geringem Schaltungsaufwand.

4 Vorteile der Erfindung

Die Kombination der zwei oben genannten Subschaltkreise bietet die folgenden Vorteile:

- Keine Interferenz von Daten verarbeitender Schaltung mit der Kommunikation;
- Schutz gegen ‚Differential Power Analysis' (DPA); sogar die elektromagnetische Abstrahlung enthält keinerlei Information, da der aufgenommene Strom der Gesamtschaltung nur von der aufgenommenen Leistung abhängt, nicht jedoch von der verarbeiteten Information ;
- Maximale Verarbeitungsleistung für die empfangene Versorgungsleistung;
- Gemessen an der konventionellen synchronen Implementation ist nur ein kleinerer Kondensator für die Filterung der Versorgungsenergie erforderlich.
- Benutzung der asynchronen Logik zur Vermeidung von korrelierbaren Mustern auf der Versorgungsleitung.
- Die vorliegende Erfindung verschleiert die Zeitbereiche, sowohl die der eigentlichen Berechnungen als auch die der Datenein- und Datenausgabe. Bei geeigneter Auslegung der Schaltung kann nicht mehr festgestellt werden, wann eine wirkliche Berechnung oder Ein-/Ausgabe stattfindet. Die 'Differential Power Analysis' wird so erheblich erschwert oder unmöglich gemacht.

5 Literatur zum Stand der Technik

[1] Kees v. Berkel, Handshake Circuits, Cambridge University Press, 1993, ISBN 0-521-45254-6

[2] Ad M.G. Peeters, Single-Rail Handshake Circuits, Proefschrift Technische Universiteit Eindhoven, 1996, ISBN 90-74445-28-4

[3] Hans van Gageldonk, An Asynchronous Low-Power 80C51 Microcontroller, Proefschrift Technische Universiteit Eindhoven, 1998, ISBN 90-74445-42-X